Auvik

Detect & secure customers' usage of SaaS with Auvik SaaS Management

TEKRiSQ

Case study

Challenges

- Needed a solution that fit their unique, multi-tenant requirements
- Unknown risk profile due to incomplete SaaS inventory
- Required a solution for user access & web-based software inventory controls

Solution

- Automated discovery of SaaS & web-based applications
- Advanced user security insights
- Security scoring & compliance alignment

Benefits

- Faster and more accurate customer assessments
- Deeper insights for a strategic business advantage
- Clearer view into previously unseen risks

About TEKRiSQ

TEKRiSQ is a new kind of cybersecurity company that helps small & medium-sized businesses (SMBs) make critical improvements to minimize technology risks. They help clients and trusted advisors address these issues which can be expensive and an enormous distraction to your core business.

The TEKRiSQ team is made up of knowledgeable, experienced technology professionals with strong expertise in IT, data security, software, and healthcare. They're on a mission to transform SMB cybersecurity preparedness and simplify how organizations protect themselves.

Needs & challenges

TEKRiSQ needed a software solution focused on their unique type of organization. As they work with organizations ranging in size, they require a way to instantly scan an environment, detect cyber security concerns, and provide recommendations for improvement. A multi-tenant solution that their technology team could centrally manage was essential.

Secondarily, while running their assessments, they had visibility into all of the installed software on their workstations using their traditional remote monitoring & management systems. Visibility into these applications was helpful, but they needed insight into the applications where most employees spend their time during the day: SaaS. SaaS is one of the fastest-growing pieces of IT in an organization's stack; these types of applications often introduce new & unexpected security threats. TEKRiSQ needed to map out a customer's software to truly understand their customer's environment.

Finally, TEKRiSQ needed a solution to help them discuss cybersecurity compliance with their customers. Whether it was HIPAA, PCI, CMMC, or any other compliance control groups, they needed something that could help check the box around user access & software access controls. Their clients not only needed the inventory & access logs to understand usage but to have a pathway toward removing unwanted and unsanctioned Shadow IT.

> **The most valuable feature is identifying the various usernames used to log into apps that are critical in terms of data security. The visibility into logs is excellent. It tells you precisely which systems or applications folks are logging into, what usernames they're using, and whether they're using single sign-on. The reporting is essential, whether defined as the reports or the APIs to get the data out. ”**

Solution in detail

Automated SaaS discovery of SaaS & web-based applications

TEKRiSQ, a one-stop-shop and all-encompassing provider of cyber-security services, required a toolset to detect their customer's environments' usage of SaaS applications.

TEKRiSQ initially relied on surveying employees with web forms to identify SaaS usage. TEKRiSQ's CEO, Dean Mechlowitz, stated that only 20% of employees would ever complete these surveys, as they were not perceived as a priority. Even more so, these surveys were, at best, 50% accurate in identifying SaaS tool usage. This would leave a massive gap in data that TEKRiSQ relied on for building a security plan around standardizing SSO and MFA. Employees would not remember to include unpaid SaaS or software they used with personal credentials. Many applications that were not self-reported were those of high & critical risk that pose significant business continuity risks to the organization.

Auvik SaaS Management enabled TEKRiSQ to gain centralized visibility and secure control over all SaaS applications & services on the market today. By monitoring the client's SaaS environment 24/7, TEKRiSQ could configure alerts about any unauthorized or high-risk applications used by employees or contractors so they could take corrective action immediately.

Advanced user insights

"Without [Auvik SaaS Management], you have zero visibility into how employees use company infrastructure. Companies will set a policy. For example, they'll make all employees use Google Drive for document storage, but employees might use their personal credentials with Google Drive or use Office SharePoint, DropBox, etc. We don't know if those systems have multifactor authentication and strong passwords. It's vital to understand what people are using because employees doing their own thing aren't doing it securely most of the time," said Dean.

Usage of shadow IT file-sharing tools, productivity tools, and document systems ran rampant, and many times each of these tools housed the most critical and sensitive business information. However, other alarming issues were found, such as how employees were accessing these tools.

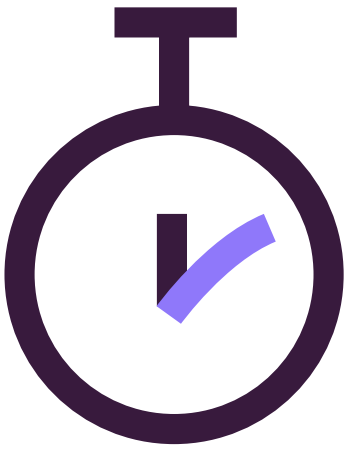
These shadow IT applications are often offenders for shared and generic accounts. Shared and generic accounts are special accounts that multiple employees access with shared username/password combinations. In many cases, this is to circumvent the need for IT to make a licensing purchase. By analyzing the usernames entered into these SaaS tools across the company, Auvik SaaS Management helped TEKRiSQ identify additional areas for increasing the environment's security posture.

Security scoring & compliance alignment

With one of TEKRiSQ's major goals being to understand how far an organization has deviated from compliance, Auvik SaaS Management drives visibility required to meet many industry-standard compliance requirements. Establishing and maintaining a software inventory for their customers allowed for advanced management with the assignment of responsible stakeholders. This created a list of authorized & unauthorized software, and with the username capture component, Auvik SaaS Management was able to help TEKRiSQ establish and maintain an inventory of accounts- a critical area that TEKRiSQ and their clients needed more visibility into.

Overall, Auvik SaaS Management helped TEKRiSQ with six critical sections of CIS Controls:

- 2.1) Establish and Maintain a software inventory
- 2.3) Address unauthorized software
- 2.5) Allowlist authorized software
- 5.1) Establish and maintain an Inventory of accounts
- 5.5) Establish and maintain an inventory of service accounts
- 9.1) Ensure use of only fully supported browsers and email clients



What is Auvik SaaS Management for TEKRiSQ?

"It's an integral part of what we want to do with our clients. Employees often do the wrong thing, and they'll continue to do the wrong things unless you can have a big bright flashlight on those things. [Auvik SaaS Management] tells us which systems people are using. It's a problem if they're outside the scope of the standard system provided by the company. That's crucial because employees don't necessarily protect their own systems adequately."

Dean Mechlowitz,
Chief Executive Officer

Key benefits

Faster and more accurate customer assessments
With an employee-driven SaaS inventory, TEKRiSQ was able to displace guesswork & manual surveys, reducing time spent on assessments.

Deeper insights for a strategic business advantage
Knowing insights beyond what is being used, such as shared & generic accounts, allowed TEKRiSQ to tighten up critical business security issues.

Clearer view into previously unseen risks
While most businesses are unaware of the risks that Shadow IT can introduce, TEKRiSQ can now shine a light and continually improve their security posture.